DoD Cyber Crime Center

A Federal Cyber Center

DC3 and the DIB:

Collaborating to Secure the Defense Ecosystem

Mr. Terry Kalka
Director, DC3/DCISE

Agenda

- About the DoD Cyber Crime Center
- Perspective on the Defense Industrial Base
- DoD's DIB CS Program
- The Role of DCISE
- Cyber Incident Reporting

DC3

A FEDERAL CYBER CENTER

Enable insight and action in cyberspace and beyond.

DC3 MISSION

A Federal Cyber Center that delivers innovative capabilities and expertise to enable and inform law enforcement, cybersecurity, and national security partners.

What We Do

DC3 offers a range of integrated services, including cyber training, digital and multimedia forensics, vulnerability disclosure, cybersecurity support to the Defense Industrial Base, analysis and operational enablement, and advanced technical solutions and capabilities.

DoD Cyber Crime Center (DC3)

A Federal Cyber Center

Cyber Forensics Lab (CFL)

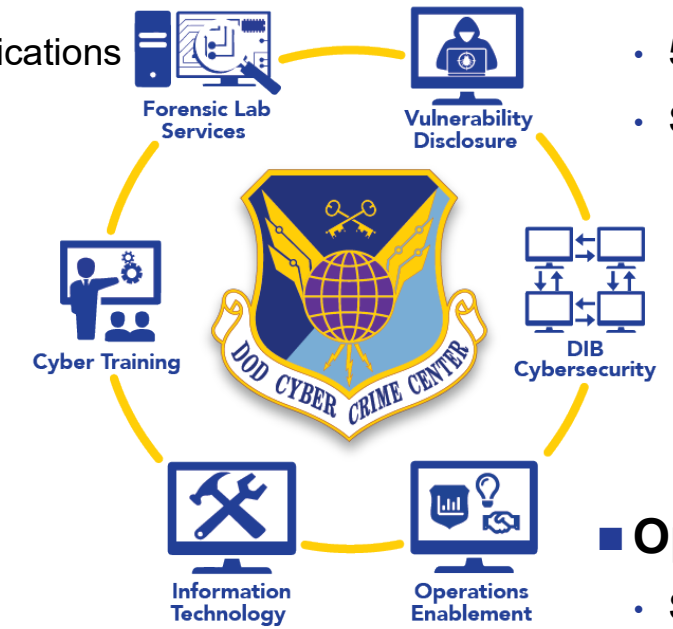
- Nationally accredited lab with exquisite digital forensics
- Support range of military operations and classifications
- Federated forensics and DC3 Pacific

Cyber Training Academy (CTA)

- In-residence, online, and mobile training teams
- Intermediate and advanced cyber courses
- LE/CI, Cyber Mission Forces, and International

Information Technology (XT)

- R&D of software and systems solutions
- Electronic Malware Submission, DC3 Advanced Carver
- Federated approach to standards, tagging, information sharing



Vulnerability Disclosure Program (VDP)

- Crowdsourced vulnerabilities on DoD systems
- 5,000 white-hat researchers from 45 countries
- Strong partnership with USCYBERCOM/JFHQ-DoDIN

Industrial Base Collaboration (DCISE)

- Cybersecurity partnership with 1,100+ CDCs
- Voluntary/mandatory DIB incident repository
- Expanded cybersecurity offerings

Operations Enablement (OED)

- Sharply focused technical/cyber intelligence analysis
- Counter FIE threats to DoD, USG, and DIB
- DoD solutions integrator in support of LE/CI/Cyber

Strategy and Partner Engagements (XE):

Deliberate partnerships to enable action - share insights - efficiently reduce risk

DoD Cyber Crime Center (DC3)

A Federal Cyber Center

SECAF is the DoD Executive Agent for DC3

- One of seven Federal Cyber Centers designated by National Security Presidential Directive (NSPD) 54 – DNI CTIIC and IC-SCC, DOJ NCIJTF, DHS CISA, DoD USCYBERCOM and NSA
- DoD Center of Excellence for digital and multimedia (D/MM) forensics, cyber training, technical solutions, research and development, cyber analytics, and vulnerability sharing

What is the DIB?

- CFR 32 pt. 236: *Defense Industrial Base (DIB*) means the Department of Defense, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

- 2022 National Defense Strategy: *The Defense Ecosystem* - the Department of Defense, the defense industrial base, and the array of private sector and academic enterprises that create and sharpen the Joint Force's technological edge.

TODAY'S ENVIRONMENT

Today's threats are more advanced and frequent than ever before

Adversaries, nonstate actors, and cyber crime organizations seek to exploit the DIB and its sensitive information

DoD relies upon the DIB to develop and produce innovative and advanced technologies, so warfighters have every available battlefield advantage

The Fundamental Problem

1. DoD provides DIB companies with sensitive, unclassified information as a necessary function
2. The DIB is targeted by advanced threats in cyberspace

3. Public/private (Government/DIB) collaboration is an essential to securing sensitive data within the DIB

DoD's DIB Cybersecurity (CS) Program

A public-private cybersecurity partnership established by DoD CIO and executed by DC3:

- Provides a collaborative environment for sharing unclassified and classified cyber threat information
- Offers analyst-to-analyst exchanges, mitigation & remediation strategies, Cybersecurity-as-a-Service
- Protects confidentiality of shared information
- Increases US Government and industry understanding of cyber threats
- **Open to Cleared Defense Contractors (through April 10, 2024)**
- **All contractors who store or process Covered Defense Information (effective April 11, 2024)**

Mission: Enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

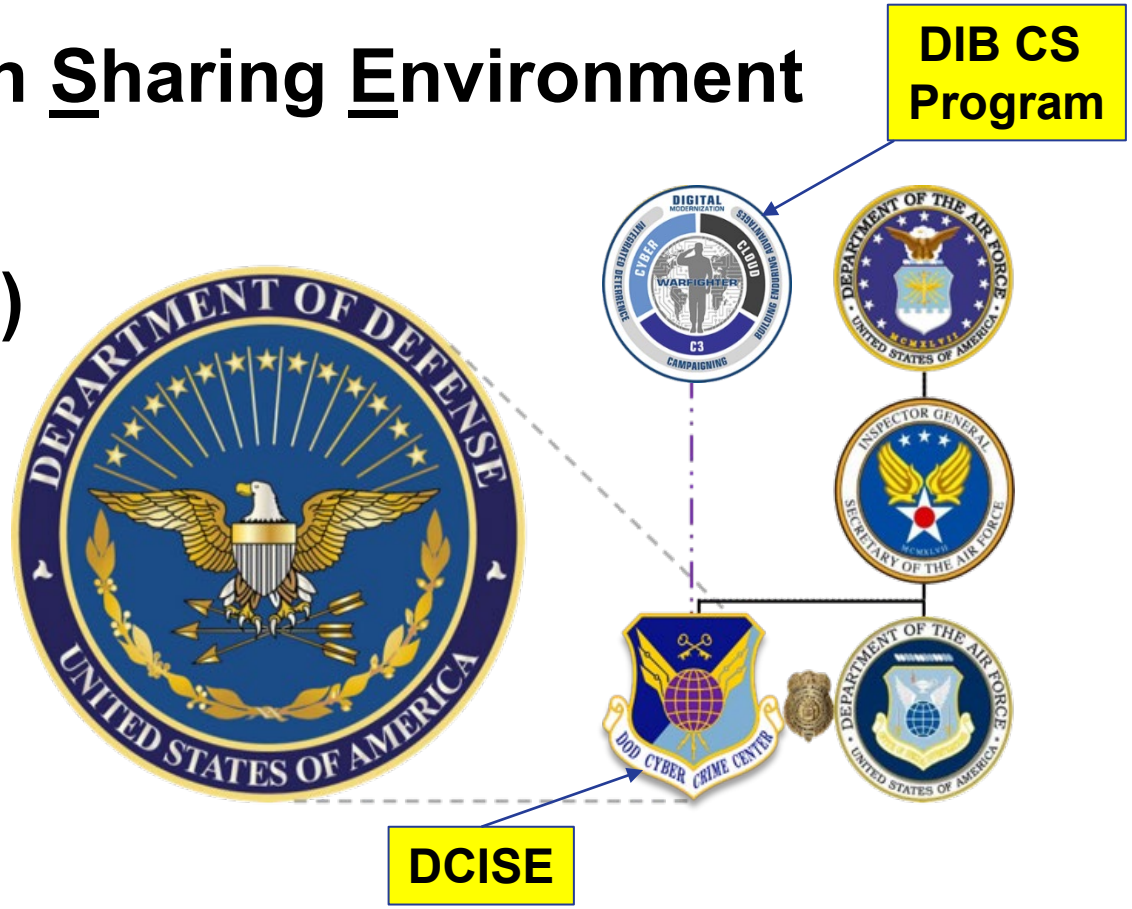
Voluntary Participation

- DIB CS Program Participants are Defense Contractors:
  - **Cleared Defense Contractors (through April 10, 2024)**
  - **All contractors who store or process Covered Defense Information (effective April 11, 2024)**
  - Large, mid, and small-sized defense contractors
  - Sole source providers, market competitors, joint-development partners, supply chain vendors
  - Manufacturers of weapon systems, platforms, and critical parts
  - Commercial Solution and Service Providers
  - Federally Funded Research and Development Centers (FFRDCs)
  - University Affiliated Research Centers (UARCs)

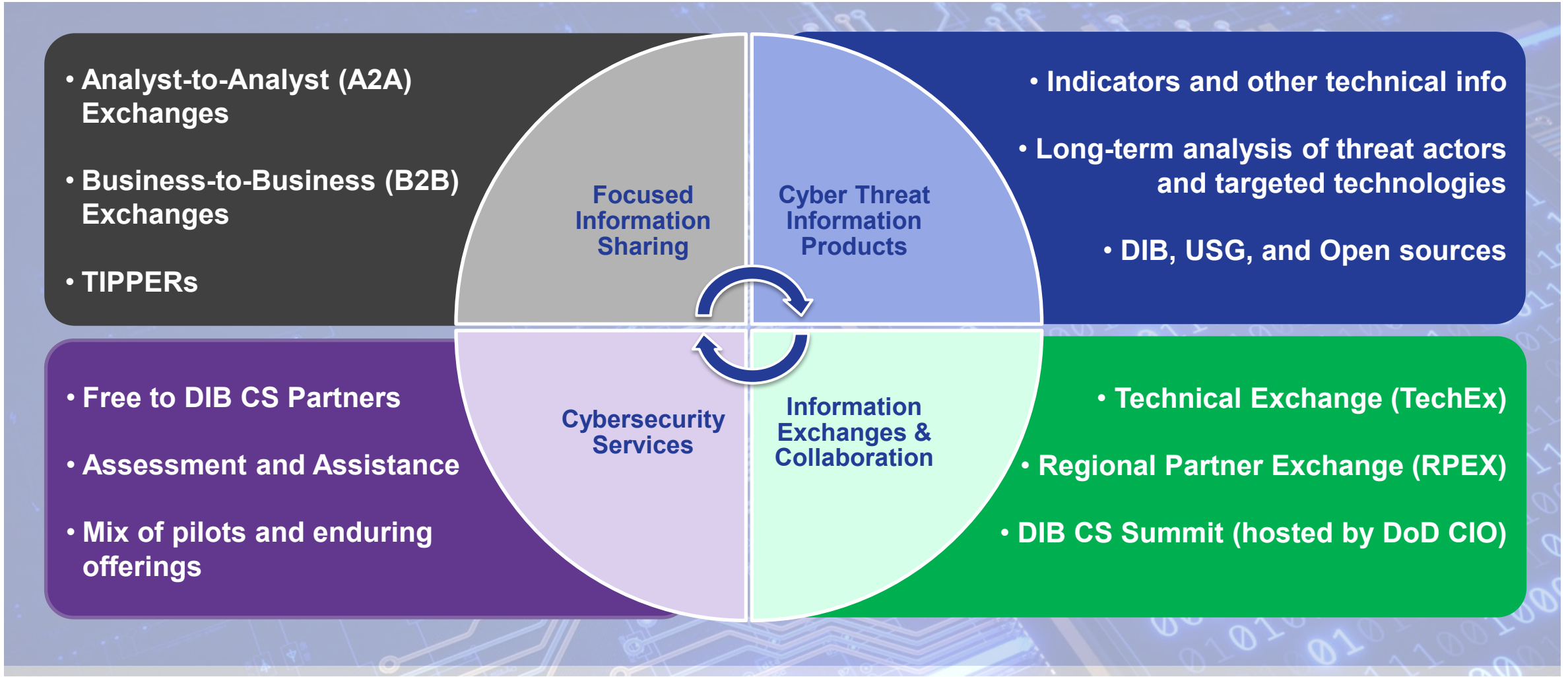
What is DCISE?

DCISE *noun* • “dice”, dīs

1. **DoD-DIB Collaborative Information Sharing Environment**
2. **A directorate within the DoD Cyber Crime Center (DC3)**
3. **The operational arm of the DIB CS Program**



DCISE Products, Services, and Activities



Cyber Resilience Analysis (CRA)

- Interview-based analysis of organization's current CS resilience posture
- Collection of 300 questions in 10 security domains
- Questions mapped to CMMC, NIST 800-171, NIST Cybersecurity Framework domains, and the Cybersecurity Framework Profile for Ransomware Risk Management
- Facilitated analysis over 6–8 hours in person or virtually
- Final report highlights strengths and weaknesses
- Partners who have repeated CRAs have seen a 90% increase in compliance for underperforming domains

DCISE³ and AET

DCISE³

- Compares DIB Partner firewall logs to DIB, USG, and commercial threat feeds
- Individual dashboards for DIB Partners
- Anonymized aggregated dashboards for DCISE analysts
- Auto-blocking feature supported on compatible firewalls
- Identified previously unknown vulnerable corporate assets
- Enabled proactive tipping to DIB Partners for instances of IOT vulnerabilities, SolarWinds compromises, Fortigate vulnerabilities, Confluence 0-days, ProxyShell targeting, malicious scanning activity
- Proved 80% uniqueness in DCISE indicators

Adversary Emulation Test (AET)

- A form of penetration testing
- Leverages adversarial tactics, techniques, and procedures
- Test of DIB Partner security controls and policies against the most likely adversary to target them

DIB-Vulnerability Disclosure Program (VDP)

- **Built on the successful 2021-2022 pilot (and the DoD-VDP)**
- **White-hat researches + Public-facing infrastructure = Vulnerabilities!**
- **Reported, validated, and sent to DIBCo for remediation**
- **Remediation validated prior to close-out**
- **Details to be announced April 2024**

Pilot Outcomes:

1019 Vulnerability Reports Total
41 Small/Medium DIB Companies
368 DIBCO Assets researched by
288 crowd-sourced ethical hackers
403 Actionable Reports, **100%** closed out

Relevant Statistics

- **Since 2008:**
  - **Conducted over 70,000 hours** of no-cost forensics and malware analysis
  - **Published over 15,000** cyber reports
  - **Shared over 610,000** actionable, non-attributional indicators
  - **80%** indicator uniqueness
- **DCISE³:**
  - **Over 262,000 high-risk IP addresses blocked**
  - **3,300,000 auto-blocked** connections
  - **213 TIPPERs** disseminated
- **CRA:**
  - **90% improvement** seen on repeat analysis
- **DIB-VDP:**
  - **403** actionable reports across 41 companies

Joining the DIB CS Program

1. Acquire an External Certification Authority (ECA) certificate* from a vendor through https://public.cyber.mil/eca/
2. Apply at https://dibnet.dod.mil/dibnet/company-application
3. Sign the Framework Agreement (+ amendments as needed)
4. Attend onboarding sessions

* - Changing from Medium Assurance Certificates to Procurement Integrated Enterprise Environment (PIEE) - *although published in the Federal Register, this change will not be immediate*

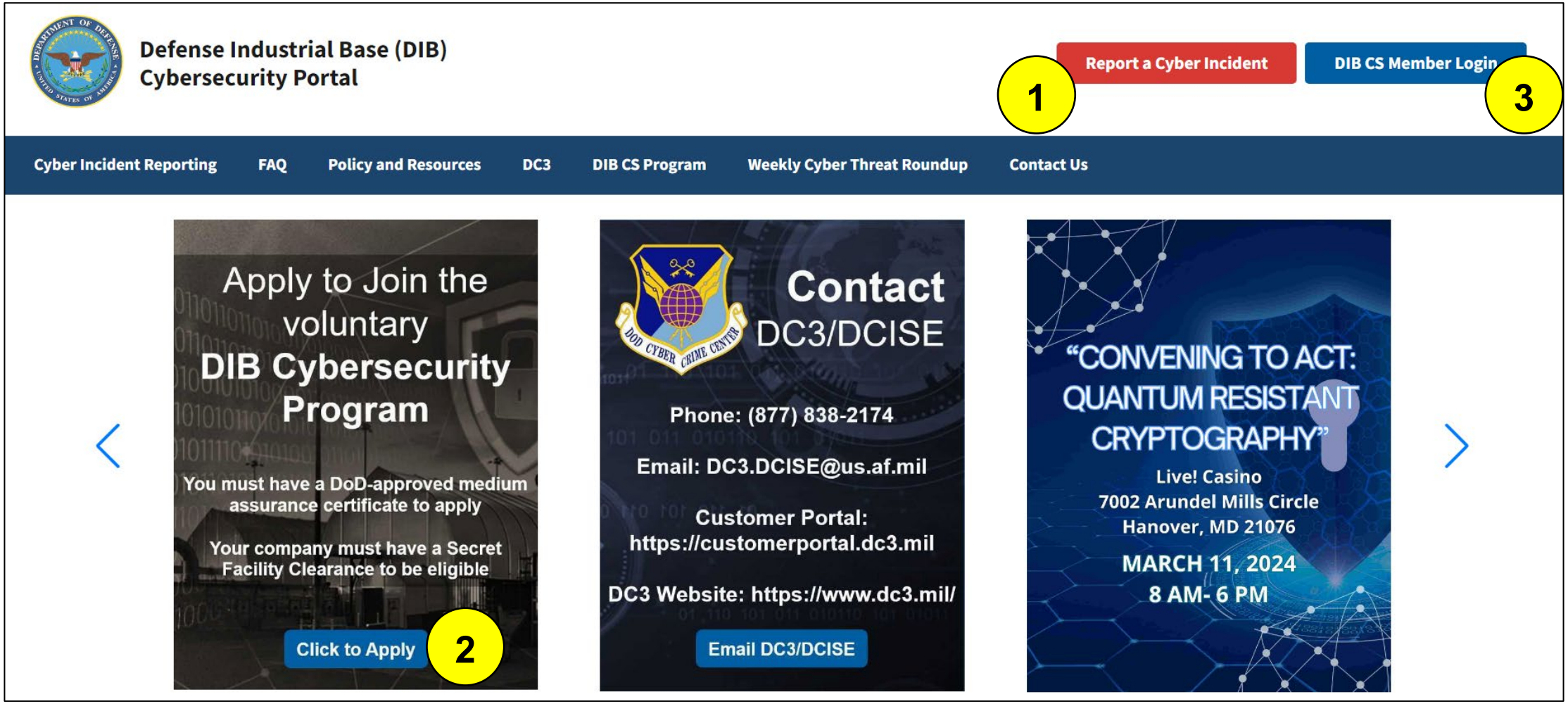
Voluntary Cyber Incident Reporting

- Mostly DIB CS Partners (although any company can report)
- Suspicious activity, or other info shareable to DIB CS Partners
- Does not rise to the level of a cyber incident under DFARS 252.204-7012
- Indicators, narrative, & analysis are *anonymized* and shared with DIB Partners & USG
- Often provides useful additional data to known incidents
- Other sources of voluntary data include Electronic Malware Submission and cybersecurity services
- Reported via Incident Collection Format (ICF) at https://dibnet.dod.mil

Mandatory Cyber Incident Reporting

- Applies to all contracts with DFARS 252.204-7012 (most DoD contracts)
- Cyber incidents affects:
  - Covered contractor information system, or
  - Covered defense information, or
  - Contractor's ability to perform operationally critical functions
- Initial report must be submitted within 72 hours of discovery
- Follow-on reports encouraged
- Affected media must be preserved for 90 days to allow for DoD to request submission
- Analysis is shared with DIB CS Partners, but may not be shared with non-partner submitters
- Cloud Service Providers to DoD report per DFARS 252.239-7010
- Reported through Incident Collection Format (ICF) at https://dibnet.dod.mil

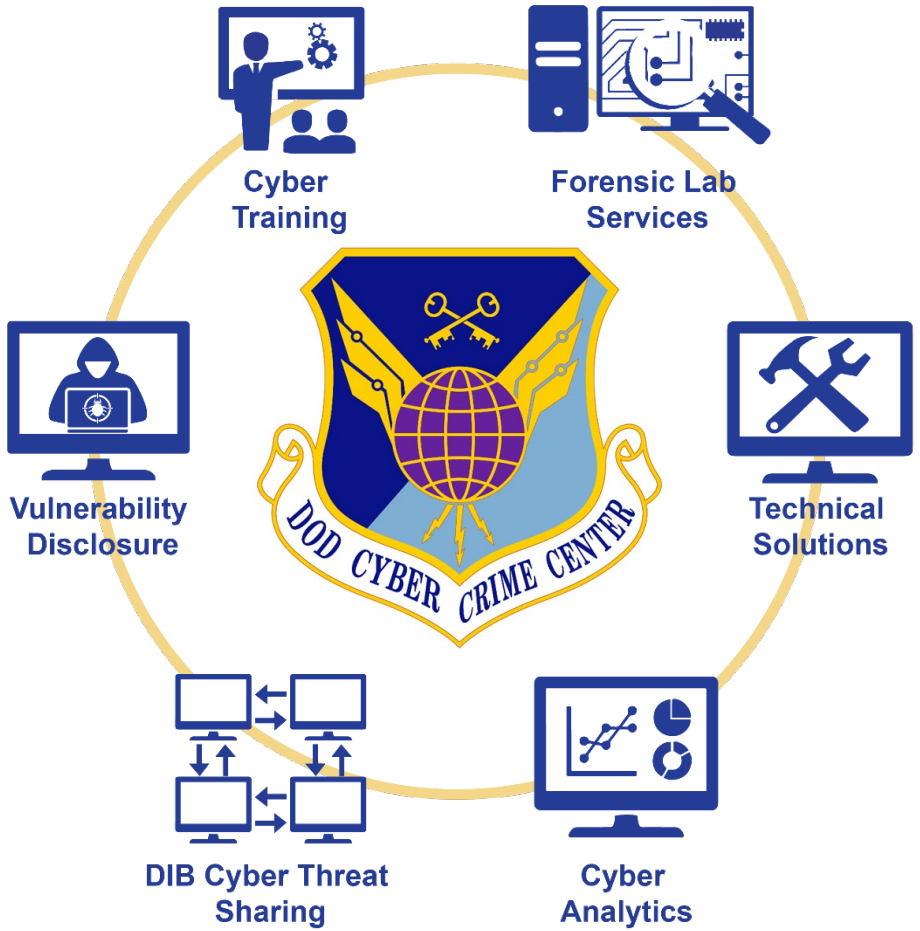
DIBNet – https://www.dibnet.dod.mil



Key Takeaways

- DIB Cybersecurity is a DoD priority
- Cyber attacks are a real and present danger to the Defense Industrial Base and to National Security
- DC3 is Federal Cyber Center and DoD Center of Excellence in digital and multimedia (D/MM) forensics, cyber training, technical solutions, research and development, cyber analytics, and vulnerability sharing
- DC3/DCISE operates the DIB CS Program in partnership with DoD CIO
- DC3 offerings are available to cleared companies, and will soon be open to all companies which store and transmit CUI
- The way ahead requires continual engagement and collaboration

Questions?



DC3 Contact info:
www.dc3.mil
410-981-6610
dc3.information@us.af.mil
on Twitter/X @DC3Forensics

DCISE (DIB-specific):
dc3.dcise@us.af.mil
410-981-0104
on Twitter/X @DC3DCISE